



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/653,804	09/01/2000	Laurence Hamid	12-51 US	5986

7590

01/24/2006

Gordon Freedman  
Freedman & Associates  
Suite 350  
117 CentrepoinTE Drive  
Nepean, ON K2G 5X3  
CANADA

EXAMINER

ABRISHAMKAR, KAVEH

ART UNIT

PAPER NUMBER

2131

DATE MAILED: 01/24/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

# Office Action Summary

Application No.

09/653,804

Applicant(s)

HAMID ET AL.

Examiner

Kaveh Abrishamkar

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

## Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

## Status

- 1) ☒ Responsive to communication(s) filed on 28 September 2005.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

## Disposition of Claims

- 4) ☒ Claim(s) 1-26 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-26 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

## Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

## Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

## Attachment(s)

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)  | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                                   | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)             |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

## **DETAILED ACTION**

### ***Continued Examination Under 37 CFR 1.114***

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on September 28, 2005 has been entered.

2. Claims 1-26 are currently being considered.

### ***Claim Objections***

3. Claim 2 is objected to because of the following informalities: "key" is misspelled "ey" in the third limitation. Appropriate correction is required.

4. Claim 19 is objected to because of the following informalities: "electronic" is misspelled "lectronic" in the third limitation. Appropriate correction is required.

### ***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

Art Unit: 2131

invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 1-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kamper (U.S. Patent No. 6,654,797) in view of Linehan et al. (U.S. Patent No. 5,495,533).

A method of restoring data of a server in communication with a communication network comprising:

providing the server for storing data, the server in communication with the communication network (Figure 1, column 2 line 53 – column 3 line 3);

providing to at least a computer in communication with the communication network, a plurality of data storage devices each having stored thereon data relating to a single authorized user (column 3 line 45 – column 4 line 13), wherein the configuration data for a server is stored on a plurality of smart cards; and

copying from each of the plurality of portable data storage devices for storage in the server, data relating to the single authorized user (column 3 line 56- column 4 line 13), wherein the configuration data is transferred from the smart cards to the server.

Kamper does not explicitly disclose that the server is a key server and that the data being stored on the server and portable storage devices is key data. Linehan discloses a computing system containing a key server which creates and stores keys which are in turn used by the user to decrypt a file (column 7 lines 30-40). Kamper and Linehan are analogous arts in that both disclose a server-centric system in which the server stores vital information which is also backed up at another destination. Linehan states that the

Art Unit: 2131

personal key server "may be replicated on multiple computers...in order to improve operational reliability" (column 6 lines 44-50). Therefore, It would have been obvious to one of ordinary skill in the art to use the backup system of Kamper to backup the key-server disclosed in Linehan "in order to improve operational reliability" (column 6 lines 47-50).

Claim 2 is rejected as applied above in rejecting claim 1. Furthermore, Kamper discloses:

A method of restoring data of a key-server in communication with a communication network as defined in claim 1, wherein the step of copying comprises:

forming a secure communication session between at least one of the plurality of portable data storage devices and the key-server (column 3 line 56 – column 4 line 13), wherein the configuration data is transferred from the smart cards to the server;

transferring the secure electronic key data via the secure communication session from the portable data storage device to the key-server (column 3 line 56 – column 4 line 13); and,

storing the transferred secure electronic key data within memory means of the key-server (column 3 line 56 – column 4 line 13).

Claim 3 is rejected as applied above in rejecting claim 2. Furthermore, Kamper discloses:

A method of restoring data of a key-server in communication with a communication network as defined in claim 2 wherein the plurality of portable data storage devices comprise all the secure electronic key data to be restored in the key-server (column 3 line 56 – column 4 line 13), wherein using the above the motivation for using the key server of Linehan with the backup system of Kamper, the configuration data being replaced in the server is view as the key data, and therefore, since Kamper discloses that the configuration data is all stored on the portable storage devices, it is asserted that the key data would be wholly stored as well.

Claim 4 is rejected as applied above in rejecting claim 3. Furthermore, Kamper discloses:

A method of restoring data of a key-server in communication with a communication network as defined in claim 3 wherein the plurality of portable data storage devices includes memory having stored therein secure electronic key data relating to each single authorized user of the communication network (column 3 lines 56 – column 4 line 13), wherein the same rationale is used above in rejecting claim 3.

Claim 5 is rejected as applied above in rejecting claim 2. Furthermore, Kamper discloses:

A method of restoring data of a key-server in communication with a communication network as defined in claim 2. Kamper does not explicitly disclose that the portable storage device includes a processor for cipher data using the stored key

and providing cryptographic functions within the portable data storage device using the secure electronic key. Linehan discloses a personal key client (smart card in case of Kamper) which encrypts data files and generates keys (column 7 lines 30-39, column 8 lines 37-45). In addition to the reasons given above for combining, it would have been obvious to provide these cryptographic functions to provide the benefits of a secure access control system as described by Linehan (column 5 lines 10-16).

Claim 6 is rejected as applied above in rejecting claim 2. Furthermore, Kamper discloses:

A method of restoring data of a key-server in communication with a communication network as defined in claim 2. Kamper does not explicitly disclose that the key server contains cryptographic functions. Linehan discloses that the key server can perform cryptographic functions such as encrypting, and creating a key (column 8 lines 37-45). In addition to the reasons given above for combining, it would have been obvious to provide these cryptographic functions to provide the benefits of a secure access control system as described by Linehan (column 5 lines 10-16).

Claim 7 is rejected as applied above in rejecting claim 6. Furthermore, Kamper discloses:

A method of restoring data of a key-server in communication with a communication network as defined in claim 6 comprising:

determining at least an available user information entry device from a plurality of known user information entry devices (column 5 lines 36-45).

receiving unique user identification information via the at least an available user information entry device (column 5 lines 35-45), wherein a user password is entered and compared at the sever; and

registering the received user identification information against security data for that user stored in the key server (column 5 lines 35-45), wherein a user password is entered and compared at the sever;

wherein the user identification information is indicative of an authorized user ciphering data is performed with secure electronic key data associated with the authorized user (column 5 lines 35-45), wherein a user password is entered and compared at the sever.

Claim 8 is rejected as applied above in rejecting claim 3. Furthermore, Kamper discloses:

A method of restoring data of a key-server in communication with a communication network as defined in claim 3 wherein each of the plurality of portable data storage devices are provided at each of a plurality of computers in communication with the network (column 5 lines 21-27).

Claim 9 is rejected as applied above in rejecting claim 8. Furthermore, Kamper discloses:



A method of restoring data of a key-server in communication with a communication network as defined in claim 8 wherein the portable data storage device is one of a token and a smart card (column 5 lines 36-45).

Claim 10 is rejected as applied above in rejecting claim 2. Furthermore, Kamper discloses:

A method of restoring data of a key-server in communication with a communication network as defined in claim 2 wherein the portable data storage device is one of a token and a smart card (column 5 lines 36-45).

Claim 11 is rejected as applied above in rejecting claim 2. Furthermore, Kamper discloses:

A method of restoring data of a key-server in communication with a communication network as defined in claim 2. Kamper does not explicitly disclose the portable storage device providing dedicated cryptographic functions for at least the computer in communication with the communication network using the security data. Linehan discloses a personal key client (smart card in case of Kamper) which encrypts data files and generates keys (column 7 lines 30-39, column 8 lines 37-45). In addition to the reasons given above for combining, it would have been obvious to provide these cryptographic functions to provide the benefits of a secure access control system as described by Linehan (column 5 lines 10-16).

Claim 12 is rejected as applied above in rejecting claim 11. Furthermore, Kamper discloses:

A method of restoring data of a key-server in communication with a communication network as defined in claim 11. Kamper does not explicitly disclose that the security data is not accessible in a useable form from outside of the key-server and the portable storage device. Linehan discloses that the key data would not be useable outside of either the key server or the portable storage device since it is encrypted (column 8 lines 18-23). It would have been obvious to use the encryption method of Linehan to encrypt the keys so that "the file encryption keys themselves do not appear in the clear on the communications path between the client and the server" (column 8 lines 18-23).

Claim 13 is rejected as applied above in rejecting claim 2. Furthermore, Kamper discloses:

A method of restoring data of a key-server in communication with a communication network as defined in claim 2. Kamper does not explicitly disclose that the key server contains cryptographic functions. Linehan discloses that the key server can perform cryptographic functions such as encrypting, and creating a key (column 8 lines 37-45). In addition to the reasons given above for combining, it would have been obvious to provide these cryptographic functions to provide the benefits of a secure access control system as described by Linehan (column 5 lines 10-16).

Regarding claim 14, Kamper discloses:

A method of backing up data of a server in communication with a communication network comprising:

providing the server in communication with the communication network, the server having stored thereon the unique user identification information for a plurality of authorized users of the communication network and the data for use by the specific authorized user in accessing data within the network (Figure 1, column 2 line 53 – column 3 line 3, column 5 lines 35-45), wherein a user password is entered and compared at the sever;

providing to at least a computer in communication with the communication network, a portable storage device (column 3 line 45 – column 4 line 13), wherein the configuration data for a server is stored on a plurality of smart cards;

receiving user identification data indicative of an authorized user of the communication network (column 5 lines 35-45), wherein a user password is entered and compared at the sever; and

copying from the server to the portable data storage device, data relating to the authorized user for use by the specified user in accessing data within the network (column 3 lines 28-35, column 5 lines 42-45), wherein the smart card retrieves the configuration so it can be used to replace the configuration of the servers at a subsequent time.

Kamper does not explicitly disclose that the server is a key server and that the data being stored on the server and portable storage devices is key data. Linehan discloses a computing system containing a key server which creates and stores keys which are in turn used by the user to decrypt a file (column 7 lines 30-40). Kamper and Linehan are analogous arts in that both disclose a server-centric system in which the server stores vital information which is also backed up at another destination. Linehan states that the personal key server "may be replicated on multiple computers...in order to improve operational reliability" (column 6 lines 44-50). Therefore, It would have been obvious to one of ordinary skill in the art to use the backup system of Kamper to backup the key-server disclosed in Linehan "in order to improve operational reliability" (column 6 lines 47-50).

Claim 15 is rejected as applied above in rejecting claim 14. Furthermore, Kamper discloses:

A method of backing up data of a key-server in communication with a communication network as defined in claim 14 wherein copying comprises:

forming a secure communication session between the key-server and the portable data storage device (column 3 line 56 – column 4 line 13), wherein the configuration data is transferred from the smart cards to the server;

transferring the secure electronic key data relating to a specific authorized user via the secure communication session from the key-server to the portable data storage device assigned to that specific authorized user (column 3 lines 28-35, column 5 lines

Art Unit: 2131

42-45), wherein the smart card retrieves the configuration so it can be used to replace the configuration of the servers at a subsequent time; and

storing the transferred secure electronic key data relating to a specific authorized user within the memory means of the portable data storage device (column 3 lines 28-35, column 5 lines 42-45).

Claim 16 is rejected as applied above in rejecting claim 15. Furthermore, Kamper discloses:

A method of backing up data of a key-server in communication with a communications network as defined in claim 15 wherein secure electronic key data specific to each of a plurality of authorized users of the communication network is stored on a separate portable data storage device assigned uniquely to one of the plurality of authorized users column 3 line 56 – column 4 line 13);

wherein the secure electronic key data of the key-server is partially stored within each portable storage device and wherein all data within the plurality of portable data storage devices is sufficient to restore security data to the key-server in the event of a data loss (column 3 line 56 – column 4 line 13), wherein using the above the motivation for using the key server of Linehan with the backup system of Kamper, the configuration data being replaced in the server is view as the key data, and therefore, since Kamper discloses that the configuration data is all stored on the portable storage devices, it is asserted that the key data would be wholly stored as well

Art Unit: 2131

Claim 17 is rejected as applied above in rejecting claim 15. Furthermore, Kamper discloses:

A method of backing up data of a key-server in communication with a communication network as defined in claim 15. Kamper does not explicitly disclose that the portable storage device includes a processor for cipher data using the stored key and providing cryptographic functions within the portable data storage device using the secure electronic key. Linehan discloses a personal key client (smart card in case of Kamper) which encrypts data files and generates keys (column 7 lines 30-39, column 8 lines 37-45). In addition to the reasons given above for combining, it would have been obvious to provide these cryptographic functions to provide the benefits of a secure access control system as described by Linehan (column 5 lines 10-16).

Claim 18 is rejected as applied above in rejecting claim 15. Furthermore, Kamper discloses:

A method of backing up data of a key-server in communication with a communication network as defined in claim 15. Kamper does not explicitly disclose that the key server contains cryptographic functions. Linehan discloses that the key server can perform cryptographic functions such as encrypting, and creating a key (column 8 lines 37-45). In addition to the reasons given above for combining, it would have been obvious to provide these cryptographic functions to provide the benefits of a secure access control system as described by Linehan (column 5 lines 10-16).

Claim 19 is rejected as applied above in rejecting claim 18. Furthermore, Kamper discloses:

A method of backing up data of a key-server in communication with a communication network as defined in claim 18, comprising:

determining at least an available user information entry device from a plurality of known user information entry devices (column 5 lines 36-45).

receiving unique user identification information via the at least an available user information entry device (column 5 lines 35-45), wherein a user password is entered and compared at the sever; and

registering the received user identification information against security data for that user stored in the key server (column 5 lines 35-45), wherein a user password is entered and compared at the sever;

wherein the user identification information is indicative of an authorized user ciphering data is performed with secure electronic key data associated with the authorized user (column 5 lines 35-45), wherein a user password is entered and compared at the sever.

Claim 20 is rejected as applied above in rejecting claim 16. Furthermore, Kamper discloses:

A method of backing up data of a key-server in communication with a communication network as defined in claim 16 wherein each of the plurality of portable

data storage devices are provided at each of a plurality of computers in communication with the network (column 5 lines 21-27).

Claim 21 is rejected as applied above in rejecting claim 20. Furthermore, Kamper discloses:

A method of backing up data of a key-server in communication with a communication network as defined in claim 8 wherein the portable data storage device is one of a token and a smart card (column 5 lines 36-45).

Claim 22 is rejected as applied above in rejecting claim 16. Furthermore, Kamper discloses:

A method of backing up data of a key-server in communication with a communication network as defined in claim 16 wherein the portable storage comprises an interface (column 5 lines 36-45).

Claim 23 is rejected as applied above in rejecting claim 15. Furthermore, Kamper discloses:

A method of backing up data of a key-server in communication with a communication network as defined in claim 15. Kamper does not explicitly disclose the portable storage device providing dedicated cryptographic functions for at least the computer in communication with the communication network using the security data. Linehan discloses a personal key client (smart card in case of Kamper) which encrypts



Art Unit: 2131

data files and generates keys (column 7 lines 30-39, column 8 lines 37-45). In addition to the reasons given above for combining, it would have been obvious to provide these cryptographic functions to provide the benefits of a secure access control system as described by Linehan (column 5 lines 10-16).

Claim 24 is rejected as applied above in rejecting claim 23. Furthermore, Kamper discloses:

A method of backing up data of a key-server in communication with a communication network as defined in claim 23. Linehan discloses that the key data would not be useable outside of either the key server or the portable storage device since it is encrypted (column 8 lines 18-23). It would have been obvious to use the encryption method of Linehan to encrypt the keys so that "the file encryption keys themselves do not appear in the clear on the communications path between the client and the server" (column 8 lines 18-23).

Claim 25 is rejected as applied above in rejecting claim 15. Furthermore, Kamper discloses:

A method of backing up data of a key-server in communication with a communication network as defined in claim 15. Kamper does not explicitly disclose that the key server contains cryptographic functions. Linehan discloses that the key server can perform cryptographic functions such as encrypting, and creating a key (column 8

lines 37-45). In addition to the reasons given above for combining, it would have been obvious to provide these cryptographic functions to provide the benefits of a secure access control system as described by Linehan (column 5 lines 10-16).

Claim 26 is rejected as applied above in rejecting claim 25. Furthermore, Kamper discloses:

A method of backing up data of a key-server in communication with a communication network as defined in claim 25. Linehan discloses that the key data would not be useable outside of either the key server or the portable storage device since it is encrypted (column 8 lines 18-23). It would have been obvious to use the encryption method of Linehan to encrypt the keys so that "the file encryption keys themselves do not appear in the clear on the communications path between the client and the server" (column 8 lines 18-23).

### ***Conclusion***


Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kaveh Abrishamkar whose telephone number is 571-272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2131

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

KA  
01/19/2006

  
AYAZ SHEIKH  
SUPERVISOR, PATENT EXAMINER  
TECHNOLOGY CENTER 2100